(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
9 October 2003 (09.10.2003)

PCT

(10) International Publication Number
WO 03/084255 A1

(51) International Patent Classification[7]: H04Q 7/00

(21) International Application Number: PCT/US03/09914

(22) International Filing Date: 28 March 2003 (28.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/112,402 29 March 2002 (29.03.2002) US

(71) Applicant *(for all designated States except US)*: **AIR-MAGNET, INC.** [US/US]; 465 Fairchild Drive, Suite 203, Mountain View, CA 94043 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **KUAN, Chia-Chee** [US/US]; 890 Lockhaven, Los Altos, CA 94024 (US). **WU, Miles** [US/US]; 231 Clara Court, Fremont, CA 94539 (US). **AU, Dean** [US/US]; 707 Koa Court, Sunnyvale, CA 94086 (US).

(74) Agents: **YIM, Peter, J.** et al.; Morrison & Foerster LLP, 425 Market Street, San Francisco, CA 94105-2482 (US).

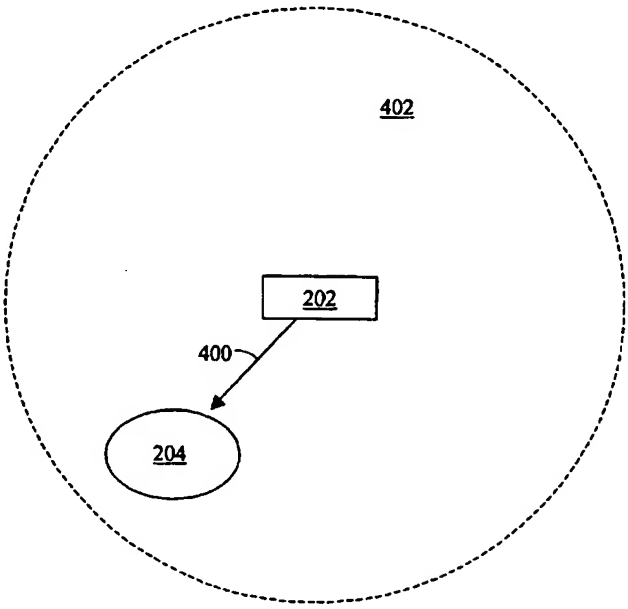
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DETECTING A COUNTERFEIT ACCESS POINT IN A WIRELESS LOCAL AREA NETWORK



(57) Abstract: In a wireless local area network, beacon frames are transmitted over the wireless LAN 200by one or more access points. The beacon frames are received in the wireless LAN 200. The received beacon frames are analyzed to detect a counterfeit access point in the wireless LAN 200.

WO 03/084255 A1

DETECTING A COUNTERFEIT ACCESS POINT IN A WIRELESS LOCAL AREA NETWORK

BACKGROUND

1. Field of the Invention

[0001] The present invention generally relates to wireless local area networks. More particularly, the present invention relates to detecting a counterfeit access point in a wireless local area network.

2. Description of the Related Art

[0002] Computers have traditionally communicated with each other through wired local area networks ("LANs"). However, with the increased demand for mobile computers such as laptops, personal digital assistants, and the like, wireless local area networks ("WLANs") have developed as a way for computers to communicate with each other through transmissions over a wireless medium using radio signals, infrared signals, and the like.

[0003] In order to promote interoperability of WLANs with each other and with wired LANs, the IEEE 802.11 standard was developed as an international standard for WLANs. Generally, the IEEE 802.11 standard was designed to present users with the same interface as an IEEE 802 wired LAN, while allowing data to be transported over a wireless medium.

[0004] Although WLANs provide users with increased mobility over wired LANs, the security of communications over a WLAN can vary for reasons that are not present in wired LANs. For instance, a counterfeit access can pose as an authorized access point in the WLAN. Stations in the WLAN can mistakenly associate with the counterfeit access point and can send confidential information to the counterfeit access point, without knowing that the counterfeit access point is unsecure. Consequently, the counterfeit access point can obtain confidential information from stations in the WLAN. Accordingly, the presence of a counterfeit access point can present security problems in a WLAN.

SUMMARY

[0005] In one embodiment of the present invention, a counterfeit access point in a wireless local area network is detected by receiving beacon frames at a detector in the wireless local area network, where the beacon frames are transmitted over the wireless local area network by one or more access points. The received beacon frames are analyzed at the detector to detect the counterfeit access point.

DESCRIPTION OF THE DRAWING FIGURES

[0006] The present invention can be best understood by reference to the following detailed description taken in conjunction with the accompanying drawing figures, in which like parts may be referred to by like numerals:

[0007] Fig. 1 shows an exemplary Open Systems Interconnection (OSI) seven layer model;

[0008] Fig. 2 shows an exemplary extended service set in a wireless local area network ("WLAN");

[0009] Fig. 3 is an exemplary flow diagram illustrating various states of stations in a WLAN;

[0010] Fig. 4 shows an exemplary embodiment of an access point sending a beacon frame;

[0011] Fig. 5 shows an exemplary embodiment of an access point and a counterfeit access point sending beacon frames;

[0012] Fig. 6 shows an exemplary flow diagram of a process for detecting a counterfeit access point in a WLAN;

[0013] Fig. 7 shows another exemplary flow diagram of a process for detecting a counterfeit access point in a WLAN; and

[0014] Fig. 8 shows another exemplary flow diagram of a process for detecting a counterfeit access point in a WLAN.

DETAILED DESCRIPTION

[0015] In order to provide a more thorough understanding of the present invention, the following description sets forth numerous specific details, such as

specific configurations, parameters, examples, and the like. It should be recognized, however, that such description is not intended as a limitation on the scope of the present invention, but is intended to provide a better description of the exemplary embodiments.

[0016] With reference to Fig. 1, an exemplary Open Systems Interconnection (OSI) seven layer model is shown, which represents an abstract model of a networking system divided into layers according to their respective functionalities. In particular, the seven layers include physical layer 102 corresponding to layer 1, data link layer 104 corresponding to layer 2, network layer 106 corresponding to layer 3, transport layer 108 corresponding to layer 4, session layer 110 corresponding to layer 5, presentation layer 112 corresponding to layer 6, and application layer 114 corresponding to layer 7. Each layer in the OSI model only interacts directly with the layer immediately above or below it, and different computers 100 and 116 can communicate directly with each other only at the physical layer 102. However, different computers 100 and 116 can effectively communicate at the same layer using common protocols. For example, in one exemplary embodiment, computer 100 can communicate with computer 116 at application layer 114 by propagating a frame from application layer 114 of computer 100 through each layer below it until the frame reaches physical layer 102. The frame can then be transmitted to physical layer 102 of computer 116 and propagated through each layer above physical layer 102 until the frame reaches application layer 114 of computer 116.

[0017] The IEEE 802.11 standard for wireless local area networks ("WLANs") operates at the data link layer 104, which corresponds to layer 2 of the OSI seven layer model, as described above. Because IEEE 802.11 operates at layer 2 of the OSI seven layer model, layers 3 and above can operate according to the same protocols used with IEEE 802 wired LANs. Furthermore, layers 3 and above can be unaware of the network actually transporting data at layers 2 and below. Accordingly, layers 3 and above can operate identically in the IEEE 802 wired LAN and the IEEE 802.11 WLAN. Furthermore, users can be presented with the same interface, regardless of whether a wired LAN or WLAN is used.

[0018] With reference to Fig. 2, an exemplary extended service set 200, which forms a WLAN according to the IEEE 802.11 standard, is depicted having basic service sets ("BSS") 206, 208, and 210. Each BSS can include an access point ("AP") 202 and stations 204. A station 204 is a component that can be used to connect to the WLAN, which can be mobile, portable, stationary, and the like, and can be referred to as the network adapter or network interface card. For instance, a station 204 can be a laptop computer, a personal digital assistant, and the like. In addition, a station 204 can support station services such as authentication, deauthentication, privacy, delivery of data, and the like.

[0019] Each station 204 can communicate directly with an AP 202 through an air link, such as by sending a radio or infrared signal between WLAN transmitters and receivers. Each AP 202 can support station services, as described above, and can additionally support distribution services, such as association, disassociation, distribution, integration, and the like. Accordingly, an AP 202 can communicate with stations 204 within its BSS 206, 208, and 210, and with other APs 202 through medium 212, called a distribution system, which forms the backbone of the WLAN. This distribution system 212 can include both wireless and wired connections.

[0020] With reference to Figs. 2 and 3, under the current IEEE 802.11 standard, each station 204 must be authenticated to and associated with an AP 202 in order to become a part of a BSS 206, 208, or 210. Accordingly, with reference to Fig. 3, a station 204 begins in State 1 (300), where station 204 is unauthenticated to and unassociated with an AP 202. In State 1 (300), station 204 can only use a limited number of frame types, such as frame types that can allow station 204 to locate and authenticate to an AP 202, and the like.

[0021] If station 204 successfully authenticates 306 to an AP 202, then station 204 can be elevated to State 2 (302), where station 204 is authenticated to and unassociated with the AP 202. In State 2 (302), station 204 can use a limited number of frame types, such as frame types that can allow station 204 to associate with an AP 202, and the like.

[0022] If station 204 then successfully associates or reassociates 308 with AP 202, then station 204 can be elevated to State 3 (304), where station 204 is authenticated to and associated with AP 202. In State 3 (304), station 204 can use any frame types to communicate with AP 202 and other stations 204 in the WLAN. If station 204 receives a disassociation notification 310, then station 204 can be transitioned to State 2. Furthermore, if station 204 then receives deauthentication notification 312, then station 204 can be transitioned to State 1. Under the IEEE 802.11 standard, a station 204 can be authenticated to different APs 202 simultaneously, but can only be associated with one AP 202 at any time.

[0023] With reference again to Fig. 2, once a station 204 is authenticated to and associated with an AP 202, the station 204 can communicate with another station 204 in the WLAN. In particular, a station 204 can send a message having a source address, a basic service set identification address ("BSSID"), and a destination address, to its associated AP 202. The AP 202 can then distribute the message to the station 204 specified as the destination address in the message. This destination address can specify a station 204 in the same BSS 206, 208, or 210, or in another BSS 206, 208, or 210 that is linked to the AP 202 through distribution system 212.

[0024] Although Fig. 2 depicts an extended service set 200 having three BSSs 206, 208, and 210, each of which include three stations 204, it should be recognized that an extended service set 200 can include any number of BSSs 206, 208, and 210, which can include any number of stations 204.

[0025] Under the current IEEE 802.11 standard, before a station 204 can associate with an AP 202, station 204 first locates the AP 202. With reference to Fig. 4, an exemplary system that can be used to locate an AP 202 using beacon frames in a WLAN is shown. More particularly, according to the current IEEE 802.11 standard, AP 202 can transmit beacon frames 400 across transmission range 402. Stations 204 located within transmission range 402 can detect beacon frames 400. In addition, stations 204 can use information in beacon frames 400 to locate AP 202's BSS 206, 208, or 210 (Fig. 2) at a later time.

[0026] Generally, beacon frames 400 can include information such as frame type, beacon frame interval/rate, sequence number, timestamp, capability information, SSID, supported rates, one or more PHY parameter sets, direct sequence (DS) parameter set, frequency hopping (FH) parameter set, and the like.

[0027] According to the current IEEE 802.11 standard, sending beacon frames 400 from AP 202 can be optional. However, some functionality in the WLAN can be lost if AP 202 does not send beacon frames 400. For instance, if AP 202 does not send beacon frames 400, station 204 may not be able to locate AP 202 by passively listening for signals from AP 202. Instead, station 204 can send a probe request to locate AP 202. However, more bandwidth and time can be required if each station 204 in the WLAN individually sends a probe request to locate AP 202. Furthermore, for roaming stations 204, if AP 202 does not send beacon frames 400 periodically, the roaming stations 204 can send probe requests periodically in order to locate the AP. However, periodically sending probe requests from these roaming stations 204 can consume even more bandwidth and time. In addition, if AP 202 does not send beacon frames 400 and station 204 does not send a probe request, then both station 204 and AP 202 can be unaware of the other. Accordingly, although sending beacon frames 400 from AP 202 can be optional, sending beacon frames 400 from AP 202 can improve the functionality of the WLAN.

[0028] However, sending beacon frames from APs in a WLAN can also compromise the security of communications over the WLAN. As noted earlier, WLANs can provide users with increased mobility, in comparison to wired LANs, but the security of communications over a WLAN can vary for reasons that are not present in wired LANs.

[0029] For instance, with reference to Fig. 5, a counterfeit AP 500 can obtain confidential information from a station 204 by posing as an authorized AP 202. More particularly, counterfeit AP 500 can transmit beacon frame 504 across a transmission range 502. Beacon frame 504 can include information such as frame type, beacon frame interval/rate, sequence number, timestamp, and the like. Stations 204 located within this transmission range 502 can detect beacon frame

504. After detecting beacon frame 504, station 204 can associate with counterfeit AP 500, without realizing that counterfeit AP 500 is not an authorized AP 202. Once associated with counterfeit AP 500, station 204 can transmit confidential information to counterfeit AP 500.

[0030] In order to avoid detection as a counterfeit AP, a counterfeit AP 500 can pose as an authorized AP 202. In particular, counterfeit AP 500 can determine information about authorized AP 202, such as the SSID for authorized AP 202, the MAC address for authorized AP 202, and the like. Counterfeit AP 500 can then be configured with the same SSID as authorized AP 202. In some applications, counterfeit AP 500 can obtain and use the MAC address of authorized AP 202. In addition, counterfeit AP 500 can locate itself near authorized AP 202 to avoid detection in the WLAN. In some applications, counterfeit AP 500 can transmit a stronger signal across the WLAN in order to entice stations 204 to associate with it instead of authorized AP 202.

[0031] Because counterfeit APs 500 can obtain confidential information from stations 204 by posing as authorized APs 202, counterfeit APs 500 can create unacceptable security problems in a WLAN. Accordingly, detecting counterfeit APs 500 in a WLAN can be used to improve security in the WLAN.

[0032] With reference to Fig. 6, an exemplary process for detecting a counterfeit AP is depicted. With reference to Fig. 5, assume for the sake of example that AP 202 is an authorized AP and that counterfeit AP 500 is an unauthorized AP attempting to pose as authorized AP 202. As described above, AP 202 sends beacon frames 400 and counterfeit AP 500 sends beacon frames 504 in an effort to associate with stations that would associate with authorized AP 202. As such, as also described above, beacon frames 504 can include similar information as beacon frames 400 in an effort to pose as beacon frames 400. For example, beacon frames 504 can have the same sender MAC address (i.e., the MAC address of authentic AP 202) and the same beacon frame rate.

[0033] In step 600 (Fig. 6) of the present exemplary process, detector 506 receives frames from APs having transmission ranges that include detector 506. As such, in the exemplary scenario depicted in Fig. 5, detector 506 receives

beacon frames 400 and 504 from authorized AP 202 and unauthorized counterfeit AP 500, respectively.

[0034] In step 602 (Fig. 6), detector 506 measures the rate at which frames are received to determine a measured frame rate. For example, in one configuration, detector 506 can count the number of beacon frames received during a period of time. For the sake of example, assume that detector 506 counts a total of 100 beacon frames, which in the exemplary scenario depicted in Fig. 5 would include beacon frames 400 and 504, during a 5 second interval. As such, in this example, the measured beacon frame rate is 20 frames per second.

[0035] In step 604 (Fig. 6), detector 506 compares the measured frame rate to the stated frame rate. As described above, the stated frame rate can be obtained from the information provided in the frame itself. In the present example, assume that the stated beacon frame rate in beacon frame 400 is 10 frames per second. As described above, the measured frame rate is 20 frames per second.

[0036] In step 606 (Fig. 6), detector 506 determines if a counterfeit AP is detected based on the comparison of the measured frame rate to the stated frame rate. Again, in the present example, the measured frame rate is 20 frames per second and the stated frame rate is 10 frames per second. As such, in the present example, detector 506 determines that a counterfeit AP has been detected based on the difference in the measured frame rate and the stated frame rate.

[0037] With reference now to Fig. 7, another exemplary process for detecting a counterfeit AP is depicted. With reference to Fig. 5, assume again that AP 202 is an authorized AP and that counterfeit AP 500 is an unauthorized AP attempting to pose as authorized AP 202. As also described above, unauthorized counterfeit AP 500 can obtain the MAC address of authorized AP 202. Counterfeit AP 500 can then use the MAC address of authorized AP 202 as the sender MAC address in beacon frames 504 in an effort to associate with stations that would associate with authorized AP 202.

[0038] In step 700 (Fig. 7) of the present exemplary process, detector 506 receives frames from APs having transmission ranges that include detector 506. As such, in the exemplary scenario depicted in Fig. 5, detector 506 receives

beacon frames 400 and 504 from authorized AP 202 and unauthorized counterfeit AP 500, respectively.

[0039] In step 702 (Fig. 7), detector 506 compares the sequence number of a received frame to the sequence number of a previously received frame with the same sender MAC address. More specifically in the present example, when detector 506 receives a beacon frame, it determines the sender MAC address of the beacon frame. If the sender MAC address of the received beacon frame matches the sender MAC address of an authorized AP, detector 506 compares the sequence number of the received beacon frame to the sequence number of a previously received beacon frame from the same authorized AP, which was stored earlier.

[0040] In step 704 (Fig. 7), detector 506 determines if a counterfeit AP is detected based on the comparison of the sequence number of the received frame to the sequence number of a previously received frame. If the sequence number of the received frame is consistent with that of the previously received frame, then detector 506 saves the sequence number of the received frame as the sequence number of a previously received frame. However, if the sequence number of the received frame is not consistent with that of the previously received frame, then detector 506 determines that a counterfeit AP has been detected.

[0041] More particularly, in accordance with current IEEE 802.11 standard, APs send frames with sequence numbers that follow an incremental pattern. For instance, assume that authorized AP 202 sends beacon frames 400 having sequence numbers in ascending order such as 100, 101, 102, and the like.

[0042] Assume that detector 506 first receives beacon frame 400 having sequence number 100. As described above, when detector 506 receives beacon frame 400, it examines the sender MAC address of beacon frame 400 to confirm that the sender MAC address matches that of an authorized AP, which in this example is that of authorized AP 202.

[0043] Assume that beacon frame 400 having sequence number 100 is the first beacon frame received from AP 202. As such, because the sequence number of the received beacon frame 400 can not be compared to that of a previously

received beacon frame 400, the sequence number of the received beacon frame 400 is stored as the new sequence number of a previously received beacon frame 400.

[0044] Now assume that detector 506 receives a beacon frame 504 from counterfeit AP 500, which is unauthorized and attempting to pose as authorized AP 202. Also assume that counterfeit AP 500 has sent beacon frame 504 using the sender MAC address of authorized AP 202. However, assume that the sequence number for beacon frame 504 sent by counterfeit AP 500 is 50. Accordingly, when detector 506 compares the sequence number of the received beacon frame, which in this example is 50, to the sequence number of the previously received beacon frame, which in this example is 100, they are not consistent. As such, detector 506 determines that a counterfeit AP 500 has been detected.

[0045] If detector 506 determines that the sequence number of the received frame and the sequence number of the previously received frame are consistent, then the sequence number of the received frame replaces the sequence number of the previously received frame, and the new sequence number is stored. For example, if the sequence number of the received frame is 101, then 506 stores 101 as the new sequence number of a previously received frame.

[0046] The IEEE 802.11 standard is a family of specifications, which includes the 802.11, 802.11a, 802.11b, and 802.11g specifications. The 802.11 specification provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). The 802.11a specification, which is an extension to the 802.11 specification, provides up to 54 Mbps in the 5GHz band using an orthogonal frequency division multiplexing encoding scheme rather than FHSS or DSSS. The 802.11b specification, which is also an extension of the 802.11 specification and commonly referred to as 802.11 High Rate or Wi-Fi, provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mpbs) in the 2.4 GHz band using DSSS. The 802.11g specification, which is the most recent extension of the 802.11 specification, provides 20+ Mbsp in the 2.4 GHz band. Undoubtedly,

further extensions and therefore additional 802.11 specifications are likely to be established and available in the future.

[0047] In accordance with the current implementation of the 802.11a specification, a total of 16 channels are defined (i.e., channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 159, 153, 157, and 161). In the US, channels 36, 40, 44, 48, 52, 56, 60, and 64 are used. In Japan, channels 34, 38, 42, and 46 are used.

[0048] In accordance with the current implementation of the 802.11b specification, a total of 14 channels are defined (i.e., channels 1-14). In the US, channels 1-11 are used. In Europe, channels 1-13 are used. In Japan, channels 1-14 are used.

[0049] With reference to Fig. 5, an authorized AP 202 operates in a single channel in a given 802.11 specification. For example, if authorized AP 202 operates using the 802.11a specification, authorized AP 202 uses one of the defined channels in the 802.11a specification (i.e., channels 34, 36, 38, 40, 42, 44, 46, 48, 52, 56, 60, 64, 159, 153, 157, and 161). Similarly, if authorized AP 202 operates using the 802.11b specification, authorized AP 202 uses one of the defined channels in the 802.11b specification (i.e., channels 1-14). Authorized AP 202 can also operate in dual-mode in which case it uses both the 802.11a and 802.11b specification. However, even in dual-mode, authorized AP 202 uses one channel in the 802.11a specification and one channel in the 802.11b specification.

[0050] With reference now to Fig. 8, another exemplary process for detecting a counterfeit AP is depicted. With reference to Fig. 5, assume again that AP 202 is an authorized AP and that counterfeit AP 500 is an unauthorized AP attempting to pose as authorized AP 202. As also described above, unauthorized counterfeit AP 500 can obtain the MAC address of authorized AP 202. Counterfeit AP 500 can then use the MAC address of authorized AP 202 as the sender MAC address in beacon frames 504 in an effort to associate with stations that would associate with authorized AP 202.

[0051] In step 800 (Fig. 8) of the present exemplary process, detector 506 receives frames from APs having transmission ranges that include detector 506.

As such, in the exemplary scenario depicted in Fig. 5, detector 506 receives beacon frames 400 and 504 from authorized AP 202 and unauthorized counterfeit AP 500, respectively.

[0052] In step 802 (Fig. 8), detector 506 determines the channels used to send the beacon frames. More specifically, when detector 506 receives beacon frames, it determines the sender MAC addresses of the beacon frames. If the sender MAC addresses of the beacon frames are the same, then detector 506 determines the channels used to send the beacon frames. In accordance with the 802.11b specification, the channel used to send the beacon frame is included in the beacon frame. Thus, detector 506 can examine the channel field in the beacon fame to determine the channel used to send the beacon frame. Alternatively, detector 506 can determine the channel on which the beacon frame was received to determine the channel used to send the beacon frame. In accordance with the 802.11a specification, the channel used to send the beacon frame is not included in the beacon frame. Thus, detector 506 can determine the channel on which the beacon frame was received to determine the channel used to send the beacon frame.

[0053] In step 804 (Fig. 8), detector 506 determines if a counterfeit AP is detected based on the channels used to send the beacon frames. More specifically, as noted above, authorized AP 202 operates using a single channel. Thus, in one embodiment, detector 506 determines that a counterfeit AP has been detected when at least two beacon frames with the same MAC addresses are detected that were sent using two different channels.

[0054] In another exemplary embodiment, detector 500 is configured to operate in multiple modes. More specifically, in a first mode, detector 506 determines that a counterfeit AP has been detected when at least two beacon frames with the same MAC addresses are detected that were sent using two different channels without regard to whether the two different channels are in different 802.11 specifications. In a second mode, detector 506 determines that a counterfeit AP has been detected when at least two beacon frames with the same MAC addresses are detected that were sent using two different channels and the two different channels are in the same 802.11 specification.

[0055] In the present exemplary embodiment, the mode in which detector 500 operates can be selected based on whether authorized AP 202 operates in dual mode. For example, if authorized AP 202 is known not to operate in dual mode, detector 500 can be selected to operate in the first mode described above (i.e., determining that a counterfeit AP has been detected when at least two beacon frames with the same MAC addresses are detected that were sent using two different channels without regard to whether the two different channels are in different 802.11 specifications). If authorized AP 202 is known to operate in dual mode, detector 500 can be selected to operate in the second mode described above (i.e., determining that a counterfeit AP has been detected when at least two beacon frames with the same MAC addresses are detected that were sent using two different channels and the two different channels are in the same 802.11 specification).

[0056] With reference to Fig. 5, the exemplary processes described above for detecting a counterfeit AP in a wireless local area network can be performed using software and/or hardware installed on a detector in the wireless local area network. In one embodiment, the detector is a station in the wireless local area network. Additionally, the station can be mobile, portable, stationary, and the like. For instance, the station can be a laptop computer, a personal digital assistant, and the like. In addition, the station can be used by a user as a diagnostic tool, by an administrator as an administrative tool, and the like, to assess the quality of communications in the WLAN.

[0057] One advantage of the present embodiment includes allowing the station to passively monitor the WLAN to detect a counterfeit AP. By passively monitoring the WLAN in this manner, the station can detect a counterfeit AP in the WLAN without burdening AP 202, consuming bandwidth, or interfering with traffic over the WLAN.

[0058] Although the present invention has been described with respect to certain embodiments, examples, and applications, it will be apparent to those skilled in the art that various modifications and changes may be made without departing from the invention.

CLAIMS

We claim:

1. A method of detecting a counterfeit access point in a wireless local area network comprising:

receiving beacon frames at a detector in the wireless local area network, wherein the beacon frames are transmitted over the wireless local area network by one or more access points; and

analyzing the received beacon frames at the detector to detect a counterfeit access point in the wireless local area network.

2. The method of claim 1, wherein analyzing comprises:

obtaining a stated beacon frame rate from a received beacon frame;

determining a measured beacon frame rate; and

comparing the measured beacon frame rate and the stated beacon frame rate.

3. The method of claim 2, wherein a counterfeit access point is detected if the measured beacon frame rate and the stated beacon frame rate are inconsistent.

4. The method of claim 2, wherein obtaining a stated beacon frame rate from the received beacon frame comprises:

examining a beacon frame to obtain a beacon frame rate stated in the beacon frame.

5. The method of claim 2, wherein determining a measured beacon frame rate comprises:

counting the number of received beacon frames during a period of time.

6. The method of claim 1, wherein analyzing comprises:

obtaining a sequence number from a received beacon frame; and

comparing the obtained sequence number to a sequence number of a previously received beacon frame.

7. The method of claim 6, wherein a counterfeit access point is detected if the obtained sequence number and the sequence number of the previously received beacon frame are inconsistent.

8. The method of claim 7, wherein a counterfeit access point is detected if the obtained sequence number and the sequence number of the previously received beacon frame are not sequential.

9. The method of claim 6 comprising:

replacing the sequence number of the previously received beacon frame with the obtained sequence number if the obtained sequence number and the sequence number of the previously received beacon frame are consistent.

10. The method of claim 6, wherein the sequence number of the previously received beacon frame is associated with a medium access control (MAC) address of the previously received beacon frame, and wherein analyzing comprises:

obtaining a sender MAC address of the received beacon frame; and

comparing the sequence number of the received beacon frame to the sequence number of the previously beacon frame if the obtained MAC address is the same as the MAC address associated with the sequence number of the previously received beacon frame.

11. The method of claim 1, wherein analyzing comprises:

determining a sender MAC address of a first received beacon frame;

determining a channel number used to send the first received beacon frame;

determining a sender MAC address of a second received beacon frame;

determining a channel number used to send the second received beacon frame; and

when the sender MAC addresses of the first and second received beacon frames are the same, comparing the determined channel numbers used to send the first and second beacon frames.

12. The method of claim 11, wherein a counterfeit access point is detected if the determined channel numbers are different.

13. The method of claim 11, wherein the beacon frames were sent using a 802.11 specification, and wherein a counterfeit access point is detected if the determined channel numbers are different and the channel numbers are in the same 802.11 specification.

14. The method of claim 13, wherein the 802.11 specification is a 802.11a specification or a 802.11b specification.

15. The method of claim 1, wherein the beacon frames are received below a network layer in an Open Systems Interconnection (OSI) model.

16. The method of claim 1, wherein the beacon frames are sent and received according to the IEEE 802.11 standard.

17. The method of claim 1, wherein the detector is a station in the wireless local area network.

18. A method of detecting a counterfeit access point in a wireless local area network comprising:

receiving beacon frames transmitted over the wireless local area network;

examining a received beacon frame to obtain a stated beacon frame rate;

determining a measured beacon frame rate; and

comparing the measured beacon frame rate and the stated beacon frame rate to detect a counterfeit access point in the wireless local area network.

19. The method of claim 18, wherein a counterfeit access pint is detected if the measured beacon frame rate and the stated beacon frame rate are not consistent.

20. The method of claim 19, wherein a counterfeit access point is detected if the measured beacon frame rate and the stated beacon frame rate are different.

21. The method of claim 18, wherein determining a measured beacon frame rate comprises:

counting the number of received beacon frames during a period of time.

22. The method of claim 18, wherein the beacon frames are received, the received beacon frame is examined, the measured beacon rate is determined, and the measured beacon frame rate and the stated beacon frame rate are compared at a detector connected to the wireless local area network.

23. The method of claim 22, wherein the detector is a station.

24. A method of detecting a counterfeit access point in a wireless local area network comprising:

receiving a beacon frame transmitted over the wireless local area network, wherein the beacon frame includes a sequence number; and

comparing the sequence number of the received beacon frame to a sequence number of a previously received beacon frame to detect a counterpart access point in the local area network.

25. The method of claim 24, wherein a counterfeit access point is detected if the sequence number of the received beacon frame and the sequence number of the previously received beacon frame are not sequential.

26. The method of claim 25 comprising:

replacing the sequence number of the previously received beacon frame with the sequence number of the received beacon frame if the sequence number of the received beacon frame and the sequence number of the previously received beacon frame are sequential.

27. The method of claim 26 comprising:

storing the sequence number of the previously received beacon frame after replacing the sequence number of the previously received beacon frame with the sequence number of the received beacon frame.

28. The method of claim 24, wherein the received beacon frame includes a medium access control (MAC) address, and wherein the sequence number of the previously received beacon frame is associated with a MAC address of the previously received beacon frame, and wherein analyzing comprises:

obtaining a sender MAC address of the received beacon frame; and

comparing the sequence number of the received beacon frame to the sequence number of the previously beacon frame if the MAC address of the received beacon frame is the same as the MAC address of the previously received beacon frame.

29. A method of detecting a counterfeit access point in a wireless local area network comprising:

receiving beacon frames transmitted over the wireless local area network;

determining a sender MAC address of a first received beacon frame;

determining a channel number used to send the first received beacon frame;

determining a sender MAC address of a second received beacon frame;

determining a channel number used to send the second received beacon frame; and

when the sender MAC addresses of the first and second received beacon frames are the same, comparing the determined channel numbers used to send the first and second beacon frames to detect a counterfeit access point in the wireless local area network.

30. The method of claim 29, wherein a counterfeit access point is detected if the determined channel numbers are different.

31. The method of claim 29, wherein the beacon frames were sent using a 802.11 specification, and wherein a counterfeit access point is detected if the determined channel numbers are different and the channel numbers are in the same 802.11 specification.

32. The method of claim 31, wherein the 802.11 specification is a 802.11a specification or a 802.11b specification.

33. An apparatus for detecting a counterfeit access point in a wireless local area network comprising:

a detector in the wireless location area configured to:

receive beacon frames transmitted over the wireless local area network; and

analyze the received beacon frames to detect a counterfeit access point in the wireless local area network.

34. The apparatus of claim 33, wherein the detector is configured to:

examine a received beacon frame to obtain a stated beacon frame;

measure a beacon frame rate; and

compare the measured beacon frame rate and the stated beacon frame rate.

35. The apparatus of claim 34, wherein the detector is configured to count the number of received beacon frames during a period of time to measure a beacon frame rate.

36. The apparatus of claim 33, wherein the detector is configured to:

examine a received beacon frame to obtain a sequence number for the received beacon frame; and

compare the obtained sequence number to a sequence number of a previously received beacon frame.

37. The apparatus of claim 36, wherein the sequence number of the previously received beacon frame is associated with a medium access control (MAC) address of the previously received beacon frame, and wherein the detector is configured to:

obtain a sender MAC address of the received beacon frame; and

compare the sequence number of the received beacon frame to the sequence number of the previously beacon frame if the obtained MAC address is the same as the MAC address associated with the sequence number of the previously received beacon frame.

38. The apparatus of claim 33, wherein the detector receives the beacon frames below a network layer in an Open Systems Interconnection (OSI) model.

39. The apparatus of claim 33, wherein the detector is a station in the wireless local area network.

40. The apparatus of claim 33, wherein the detector is configured to:

determine a sender MAC address of a first received beacon frame;

determine a channel number used to send the first received beacon frame;

determine a sender MAC address of a second received beacon frame;

determine a channel number used to send the second received beacon frame; and

when the sender MAC addresses of the first and second received beacon frames are the same, compare the determined channel numbers used to send the first and second beacon frames.

41. The apparatus of claim 40, wherein a counterfeit access point is detected if the determined channel numbers are different.

42. The apparatus of claim 40, wherein the beacon frames were sent using a 802.11 specification, and wherein a counterfeit access point is detected if the determined channel numbers are different and the channel numbers are in the same 802.11 specification.

43. The apparatus of claim 42, wherein the 802.11 specification is a 802.11a specification or a 802.11b specification.

44. A computer-readable storage medium containing computer executable code to detect a counterfeit access point in a wireless local area network by instructing the computer to operate as follows:

receiving beacon frames transmitted over the wireless local area network at a station in the wireless local area network; and

analyzing the received beacon frames at the station to detect a counterfeit access point in the wireless local area network.

45. The computer-readable storage medium of claim 44, wherein analyzing comprises:

obtaining a stated beacon frame rate from a received beacon frame;

determining a measured beacon frame rate; and

comparing the measured beacon frame rate and the stated beacon frame rate.

46. The computer-readable storage medium of claim 45, wherein determining a measured beacon frame rate comprises:

counting the number of received beacon frames during a period of time.

47. The computer-readable storage medium of claim 44, wherein analyzing comprises:

obtaining a sequence number from a received beacon frame; and

comparing the obtained sequence number to a sequence number of a previously received beacon frame.

48. The computer-readable storage medium of claim 47, wherein a counterfeit access point is detected if the obtained sequence number and the sequence number of the previously received beacon frame are not sequential.

49. The computer-readable storage medium of claim 47 comprising:

replacing the sequence number of the previously received beacon frame with the obtained sequence number if the obtained sequence number and the sequence number of the previously received beacon frame are consistent.

50. The computer-readable storage medium of claim 47, wherein the sequence number of the previously received beacon frame is associated with a medium access control (MAC) address of the previously received beacon frame, and wherein analyzing comprises:

obtaining a sender MAC address of the received beacon frame; and

comparing the sequence number of the received beacon frame to the sequence number of the previously beacon frame if the obtained MAC address is the same as the MAC address associated with the sequence number of the previously received beacon frame.

51. The computer-readable storage medium of claim 44, wherein analyzing comprises:

determining a sender MAC address of a first received beacon frame;

determining a channel number used to send the first received beacon frame;

determining a sender MAC address of a second received beacon frame;

determining a channel number used to send the second received beacon frame; and

when the sender MAC addresses of the first and second received beacon frames are the same, comparing the determined channel numbers used to send the first and second beacon frames.

52. The computer-readable storage medium of claim 51, wherein a counterfeit access point is detected if the determined channel numbers are different.

53. The computer-readable storage medium of claim 51, wherein the beacon frames were sent using a 802.11 specification, and wherein a counterfeit access point is detected if the determined channel numbers are different and the channel numbers are in the same 802.11 specification.

54. The computer-readable storage medium of claim 53, wherein the 802.11 specification is a 802.11a specification or a 802.11b specification.

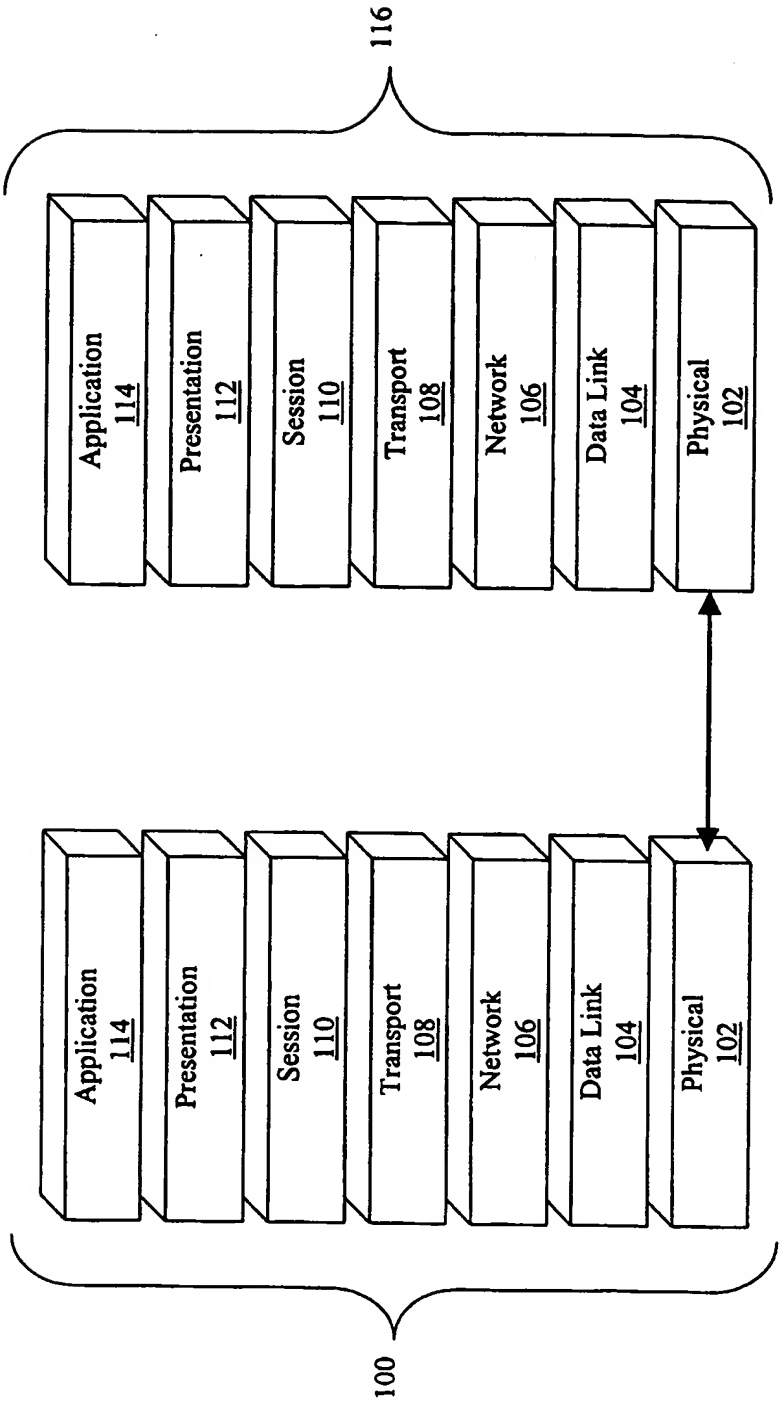

116
Application 114
Presentation 112
Session 110
Transport 108
Network 106
Data Link 104
Physical 102
Application 114
Presentation 112
Session 110
Transport 108
Network 106
Data Link 104
Physical 102
100

Fig. 1

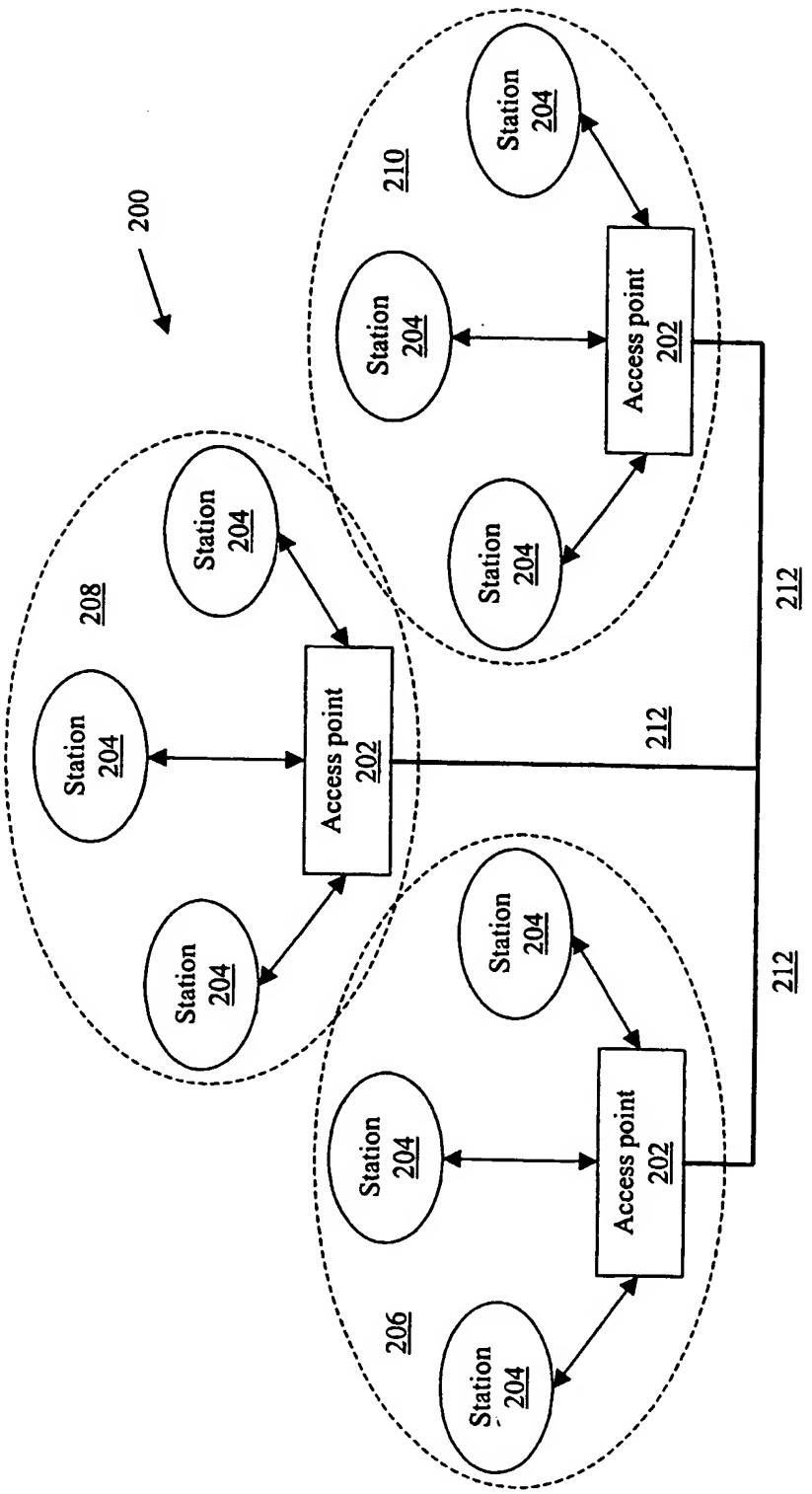


Fig. 2

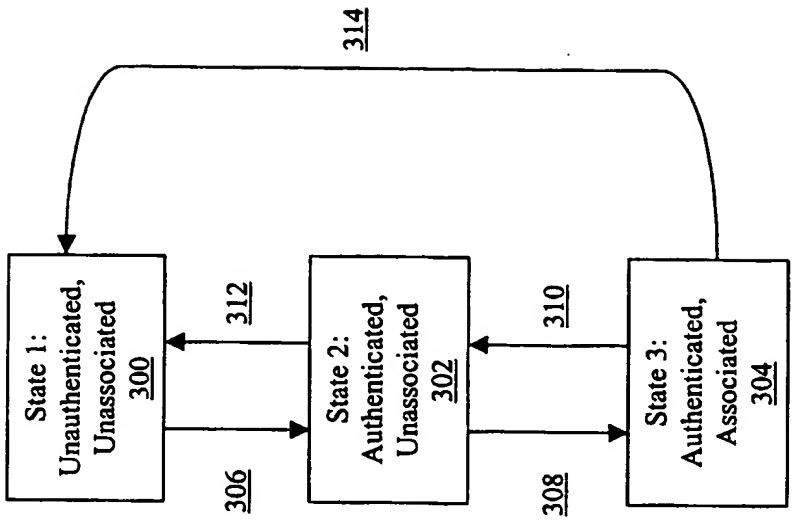

314
State 1: Unauthenticated, Unassociated 300
State 2: Authenticated, Unassociated 302
State 3: Authenticated, Associated 304
312
310
306
308

Fig. 3

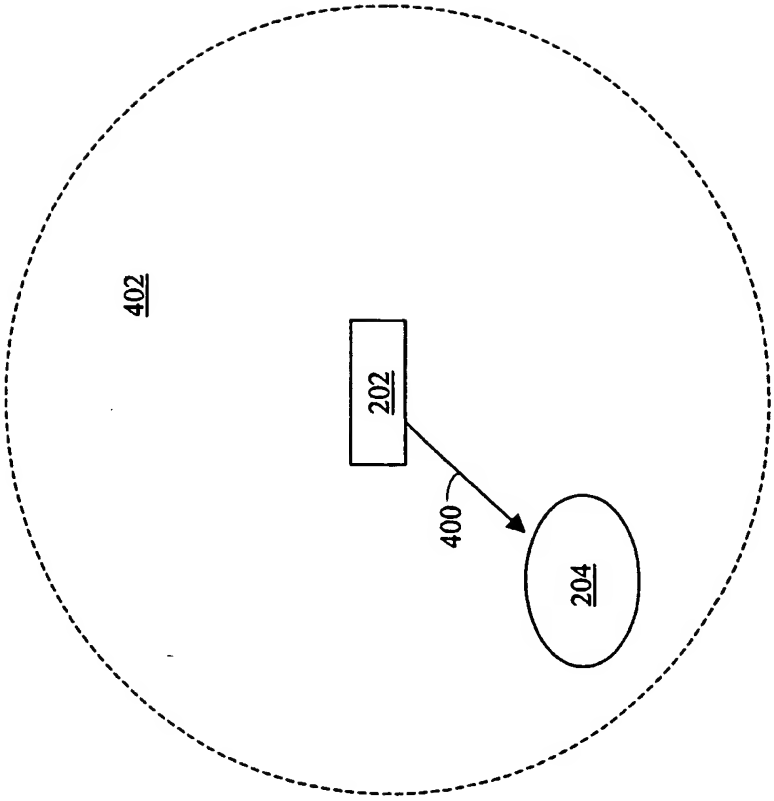


Fig. 4

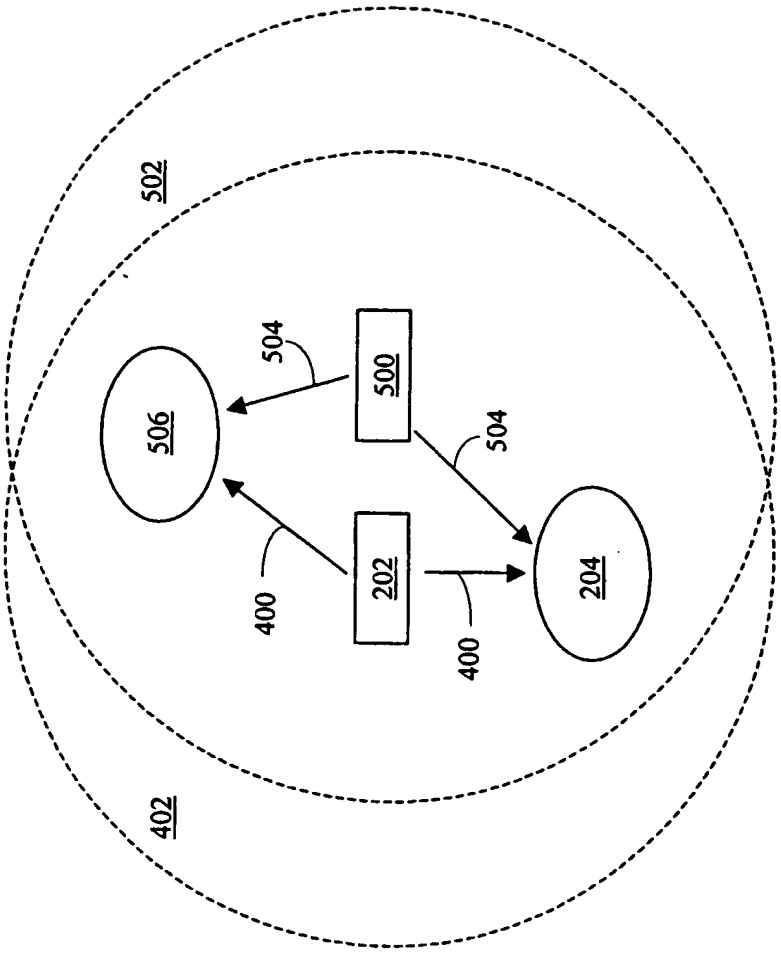


Fig. 5

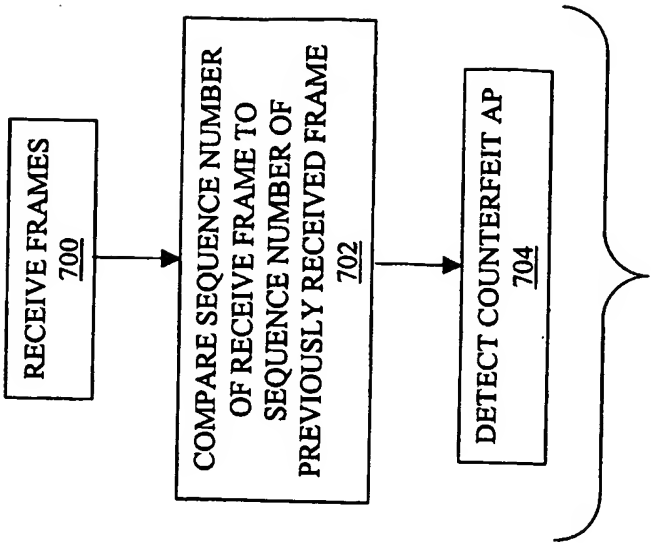

RECEIVE FRAMES
700
COMPARE SEQUENCE NUMBER OF RECEIVE FRAME TO SEQUENCE NUMBER OF PREVIOUSLY RECEIVED FRAME
702
DETECT COUNTERFEIT AP
704

Fig. 7

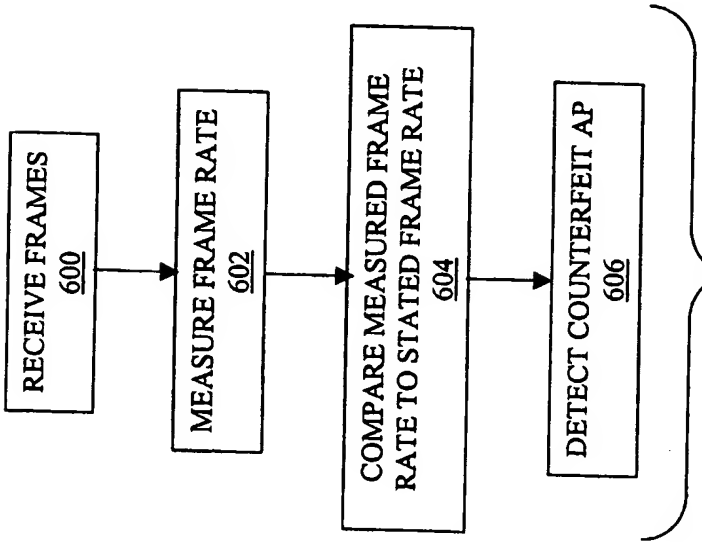

RECEIVE FRAMES
600
MEASURE FRAME RATE
602
COMPARE MEASURED FRAME RATE TO STATED FRAME RATE
604
DETECT COUNTERFEIT AP
606

Fig. 6

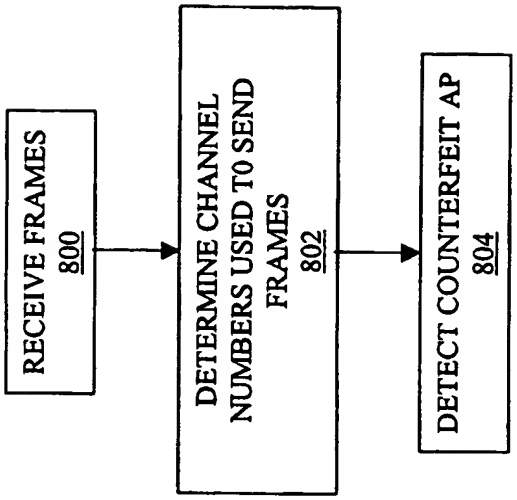

RECEIVE FRAMES
800
DETERMINE CHANNEL NUMBERS USED TO SEND FRAMES
802
DETECT COUNTERFEIT AP
804

Fig. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/09914

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) :H04Q 7/00
US CL : 370/328
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 370/328, 338, 332, 329, 230, 221

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 6, 188,681 B1 (VESUNA) 13 February 2001, abstract, col 1 lines 12-27, 36-67, col 2 lines 20-37.	1, 15-21, 24-25, 33, 38-39, 44
Y,P	US 6,393,261 B1 (LEWIS) 21 May 2002, col 2 lines 44-65, col 5 lines 26-46	1, 15-21, 24-25, 33, 38-39, 44

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search
30 MAY 2003

Date of mailing of the international search report
18 JUN 2003

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer
RICARDO PIZARRO
Telephone No. (703) 305-4700

Form PCT/ISA/210 (second sheet) (July 1998)*

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
16 October 2003 (16.10.2003)

PCT

(10) International Publication Number
WO 03/085544 A1

(51) International Patent Classification[7]: G06F 15/173

(21) International Application Number: PCT/US03/09682

(22) International Filing Date: 28 March 2003 (28.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
10/116,473 4 April 2002 (04.04.2002) US

(71) Applicant *(for all designated States except US)*: **AIR-MAGNET, Inc.** [US/US]; 465 Fairchild Drive,, Suite 203, Mountain View, CA 94043 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **KUAN, Chia-Chee** [US/US]; 890 Lockhaven, Los Altos, CA 94024 (US). **WU, Miles** [US/US]; 231 Clara Court, Fremont, CA 94539 (US). **AU, Dean** [US/US]; 707 Koa Court, Sunnyvale, CA 94086 (US).

(74) Agents: **YIM, Peter, J.** et al.; Morrison & Foerster LLP, 425 Market Street, San Francisco, CA 94105-2482 (US).

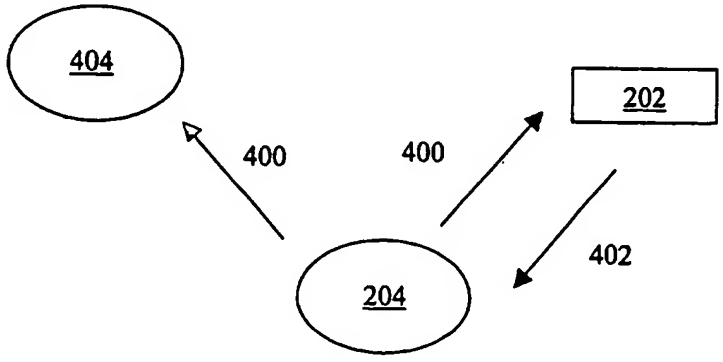
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: DETECTING AN UNAUTHORIZED STATION IN A WIRELESS LOCAL AREA NETWORK



(57) Abstract: In a wireless local area network a probe request frame (400) is transmitted over the wireless local area network by a station. The probe request frame is received at a detector (404) in the wireless local area network. The received probe request frame is analyzed to determine if the station that transmitted the probe request frame is an unauthorized station.

WO 03/085544 A1

DETECTING AN UNAUTHORIZED STATION IN A WIRELESS LOCAL AREA NETWORK

BACKGROUND

1. Field of the Invention

[0001] The present invention generally relates to wireless local area networks. More particularly, the present invention relates to detecting an unauthorized station in a wireless local area network.

2. Description of the Related Art

[0002] Computers have traditionally communicated with each other through wired local area networks ("LANs"). However, with the increased demand for mobile computers such as laptops, personal digital assistants, and the like, wireless local area networks ("WLANs") have developed as a way for computers to communicate with each other through transmissions over a wireless medium using radio signals, infrared signals, and the like.

[0003] In order to promote interoperability of WLANs with each other and with wired LANs, the IEEE 802.11 standard was developed as an international standard for WLANs. Generally, the IEEE 802.11 standard was designed to present users with the same interface as an IEEE 802 wired LAN, while allowing data to be transported over a wireless medium.

[0004] Although WLANs provide users with increased mobility over wired LANs, the security of communications over a WLAN can vary for reasons that are not present in wired LANs. For instance, an unauthorized station can scan for signals transmitted over the WLAN to obtain information about the WLAN. This type of network intrusion is commonly known as a "war driving" activity.

SUMMARY

[0005] In one embodiment of the present invention, an unauthorized station in a wireless local area network is detected by receiving a probe request at a detector in the wireless local area network, where the probe request frame was transmitted over the wireless local area network by a station. The received probe request frame is analyzed at the detector to determine if the station that transmitted the probe request frame is an unauthorized station.

DESCRIPTION OF THE DRAWING FIGURES

[0006] The present invention can be best understood by reference to the following detailed description taken in conjunction with the accompanying drawing figures, in which like parts may be referred to by like numerals:

[0007] Fig. 1 shows an exemplary OSI seven layer model;

[0008] Fig. 2 shows an exemplary extended service set in a wireless local area network ("WLAN");

[0009] Fig. 3 is an exemplary flow diagram illustrating various states of stations in a WLAN;

[0010] Fig. 4 shows an exemplary embodiment of a station sending a probe request frame;

[0011] Fig. 5 shows an exemplary process of detecting an unauthorized station and/or "war driving" activities; and

[0012] Fig. 6 shows another exemplary process of detecting an unauthorized station and/or "war driving activities.

DETAILED DESCRIPTION

[0013] In order to provide a more thorough understanding of the present invention, the following description sets forth numerous specific details, such as specific configurations, parameters, examples, and the like. It should be recognized, however, that such description is not intended as a limitation on the scope of the present invention, but is intended to provide a better description of the exemplary embodiments.

[0014] With reference to Fig. 1, an exemplary OSI seven layer model is shown, which represents an abstract model of a networking system divided into layers according to their respective functionalities. In particular, the seven layers include physical layer 102 corresponding to layer 1, data link layer 104 corresponding to layer 2, network layer 106 corresponding to layer 3, transport layer 108 corresponding to layer 4, session layer 110 corresponding to layer 5, presentation layer 112 corresponding to layer 6, and application layer 114 corresponding to layer 7. Each layer in the OSI model only interacts directly with the layer immediately above or below it, and different computers 100 and 116 can communicate directly with each other only at the physical layer 102. However, different computers 100 and 116 can effectively

communicate at the same layer using common protocols. For example, in one exemplary embodiment, computer 100 can communicate with computer 116 at application layer 114 by propagating a frame from application layer 114 of computer 100 through each layer below it until the frame reaches physical layer 102. The frame can then be transmitted to physical layer 102 of computer 116 and propagated through each layer above physical layer 102 until the frame reaches application layer 114 of computer 116.

[0015] The IEEE 802.11 standard for wireless local area networks ("WLANs") operates at the data link layer 104, which corresponds to layer 2 of the OSI seven layer model, as described above. Because IEEE 802.11 operates at layer 2 of the OSI seven layer model, layers 3 and above can operate according to the same protocols used with IEEE 802 wired LANs. Furthermore, layers 3 and above can be unaware of the network actually transporting data at layers 2 and below. Accordingly, layers 3 and above can operate identically in the IEEE 802 wired LAN and the IEEE 802.11 WLAN. Furthermore, users can be presented with the same interface, regardless of whether a wired LAN or WLAN is used.

[0016] With reference to Fig. 2, an exemplary extended service set 200, which forms a WLAN according to the IEEE 802.11 standard, is depicted having basic service sets ("BSS") 206, 208, and 210. Each BSS can include an access point ("AP") 202 and stations 204. A station 204 is a component that can be used to connect to the WLAN, which can be mobile, portable, stationary, and the like, and can be referred to as the network adapter or network interface card. For instance, a station 204 can be a laptop computer, a personal digital assistant, and the like. In addition, a station 204 can support station services such as authentication, deauthentication, privacy, delivery of data, and the like.

[0017] Each station 204 can communicate directly with an AP 202 through an air link, such as by sending a radio or infrared signal between WLAN transmitters and receivers. Each AP 202 can support station services, as described above, and can additionally support distribution services, such as association, disassociation, distribution, integration, and the like. Accordingly, an AP 202 can communicate with stations 204 within its BSS 206, 208, and 210, and with other APs 202 through medium 212, called a distribution system, which forms the backbone of the WLAN. This distribution system 212 can include both wireless and wired connections.

[0018] With reference to Figs. 2 and 3, under the current IEEE 802.11 standard, each station 204 must be authenticated to and associated with an AP 202 in order to become a part of a BSS 206, 208, or 210. Accordingly, with reference to Fig. 3, a station 204 begins in State 1 (300), where station 204 is unauthenticated to and unassociated with an AP 202. In State 1 (300), station 204 can only use a limited number of frame types, such as frame types that can allow station 204 to locate and authenticate to an AP 202, and the like.

[0019] If station 204 successfully authenticates 306 to an AP 202, then station 204 can be elevated to State 2 (302), where station 204 is authenticated to and unassociated with the AP 202. In State 2 (302), station 204 can use a limited number of frame types, such as frame types that can allow station 204 to associate with an AP 202, and the like.

[0020] If station 204 then successfully associates or reassociates 308 with AP 202, then station 204 can be elevated to State 3 (304), where station 204 is authenticated to and associated with AP 202. In State 3 (304), station 204 can use any frame types to communicate with AP 202 and other stations 204 in the WLAN. If station 204 receives a disassociation notification 310, then station 204 can be transitioned to State 2. Furthermore, if station 204 then receives deauthentication notification 312, then station 204 can be transitioned to State 1. Under the IEEE 802.11 standard, a station 204 can be authenticated to different APs 202 simultaneously, but can only be associated with one AP 202 at any time.

[0021] With reference again to Fig. 2, once a station 204 is authenticated to and associated with an AP 202, the station 204 can communicate with another station 204 in the WLAN. In particular, a station 204 can send a message having a source address, a basic service set identification address ("BSSID"), and a destination address, to its associated AP 202. The AP 202 can then distribute the message to the station 204 specified as the destination address in the message. This destination address can specify a station 204 in the same BSS 206, 208, or 210, or in another BSS 206, 208, or 210 that is linked to the AP 202 through distribution system 212.

[0022] Although Fig. 2 depicts an extended service set 200 having three BSSs 206, 208, and 210, each of which include three stations 204, it should be recognized that an extended service set 200 can include any number of BSSs 206, 208, and 210, which can include any number of stations 204.

[0023] Under the current IEEE 802.11 standard, before a station 204 can associate with an AP 202, station 204 first locates AP 202. With reference to Fig. 4, according to the current IEEE 802.11 standard, station 204 can transmit a probe request frame 400. Probe request frame 400 can include various element fields, such as service set identification address (SSID), supported rates, and the like. When AP 202 receives probe request frame 400, it transmits a probe response frame 402. Probe request frame 402 can include various element fields, such as timestamp, beacon interval, capability information, SSID, supported rate, channels, and the like.

[0024] If station 204 is an authorized station, meaning that it is authorized to obtain service from AP 202, it can use the information in probe response frame 402 to begin the process of autheticating or associating with AP 202. If station 204 is an unauthorized station and AP 202 is an unsecured access point, meaning that it does not have security measures to prevent unauthorized use, the unauthorized station can also associate with AP 202. Alternatively, if station 204 is an unauthorized station, it can simply store the information obtained from probe response frame 402. Additionally, the receipt of probe response frame 402 can inform an unauthorized station of the existence of AP 202, which may then be published or used in some other undesirable manner.

[0025] As noted earlier, obtaining information about AP 202 in this manner is commonly known as "war driving." One typical practice of war driving is to use a laptop or a similar portable device with a wireless network card and an antenna, and literally drive around to scan for WLAN signals.

[0026] With reference to Fig. 4, in one exemplary embodiment, a detector 404 is configured to determine whether station 204 is an unauthorized station. More specifically, detector 404 is configured to detect "war driving" activity from station 204.

[0027] In the present embodiment, detector 404 receives transmissions between AP 202 and station 204. Detector 404 then analyzes the transmissions from station 204 for "war driving" activity.

[0028] With reference to Fig. 5, an exemplary process for detecting an unauthorized station, and more particularly an unauthorized station engaging in "war driving" activity is depicted. With reference to Fig. 4, in step 500 (Fig. 5), detector 404 receives probe request frames 400 sent from station 204. In step 502 (Fig. 5), detector

404 then analyzes the probe request frames 400 for characteristics that are indicative of "war driving" activity. In step 504 (Fig. 5), if "war driving" activity is detected, detector 404 can provide an alert.

[0029] With reference to Fig. 6, an exemplary process for detecting "war driving" activity is depicted. With reference to Fig. 4, in step 600 (Fig. 6), a probe request frame 400 is examined to determine if it has a zero length SSID. In step 602 (Fig. 6), probe request frame 400 is examined to determine if it has only a SSID information element field and no other fields. In step 604 (Fig. 6), after transmitting probe response frame 402, detector 404 determines if station 204 fails to proceed with authentication or association requests.

[0030] With reference to Fig. 6, in one embodiment, if the determinations in steps 600, 602, and 604 are affirmative, meaning that probe request frame 400 is determined to have a zero length SSID and only SSID information element field and station 204 (Fig. 4) fails to proceed with authentication or association requests, then station 204 is determined to be an unauthorized station and/or engaging in "war driving" activity.

[0031] With reference to Fig. 4, the exemplary processes described above for detecting an unauthorized station and/or "war driving" activity can be performed using software and/or hardware installed on detector 404. In one embodiment, detector 404 is a station in a wireless local area network. Additionally, the station can be mobile, portable, stationary, and the like. For instance, the station can be a laptop computer, a personal digital assistant, and the like. In addition, the station can be used by a user as a diagnostic tool, by an administrator as an administrative tool, and the like, to assess the quality of communications in the WLAN.

[0032] One advantage of the present embodiment includes allowing detector 404 to passively monitor the WLAN for unauthorized stations and/or "war driving" activities. By passively monitoring the WLAN in this manner, detector 404 can detect unauthorized stations and/or "war driving" activities in the WLAN without burdening AP 202, consuming bandwidth, or interfering with traffic over the WLAN.

[0033] Although the present invention has been described with respect to certain embodiments, examples, and applications, it will be apparent to those skilled in the art that various modifications and changes may be made without departing from the invention.

CLAIMS

We claim:

1. A method of detecting an unauthorized station in a wireless local area network comprising:

receiving a probe request frame at a detector in the wireless local area network, wherein the probe request frame is transmitted over the wireless local area network by a station; and

analyzing the probe request frame received at the detector to determine if the station that transmitted the probe request frame is an unauthorized station.

2. The method of claim 1 further comprising:

receiving the probe request frame at an access point; and

sending a probe response frame from the access point.

3. The method of claim 2, wherein the probe request frame has a service set identification address ("SSID"), and wherein analyzing the probe request frame comprises:

examining the probe request frame to determine if the length of the SSID is zero;

examining the probe request frame to determine if the probe request frame only has a SSID information element field; and

determining if the station that transmitted the probe request frame fails to proceed with authentication or authorization in response to the probe response frame.

4. The method of claim 1, wherein analyzing the probe request frame comprises:

determining if the station that transmitted the probe request frame is engaging in a war driver activity.

5. The method of claim 4, wherein determining if the station is engaging in a war driver activity comprises:

determining if the probe request frame has a service set identification address ("SSID") with a length of zero;

determining if the probe request frame only has a SSID information element field; and

determining if the station that transmitted the probe request frame fails to proceed with authentication or authorization in response to a probe response frame sent from an access point.

6. The method of claim 1, wherein the probe request frame is received below a network layer in an OSI model.

7. The method of claim 1, wherein the probe request frame is sent and received according to the IEEE 802.11 standard.

8. The method of claim 1, wherein the detector is a station in the wireless local area network.

9. A method of detecting an unauthorized station in a wireless local area network engaging in "war driver" activity, the method comprising:

receiving a probe request frame sent from a station at a detector; and

analyzing the probe request frame at the detector to determine if the station that sent the probe request frame is an unauthorized station.

10. The method of claim 9, wherein analyzing the probe request frame comprises:

determining if the probe request frame has a service set identification address ("SSID") with a length of zero;

determining if the probe request frame only has a SSID information element field; and

determining if the station fails to proceed with authentication or authorization in response to a probe response frame sent from an access point.

11. The method of claim 10 further comprising:

identifying the station that sent the probe request frame as an unauthorized station if the probe request frame has a SSID length of zero, the probe request frame

only has a SSID information element frame, and the station fails to proceed with authentication or authorization in response to a probe response frame.

12. The method of claim 10 further comprising:

identifying the station that sent the probe request frame as engaging in "war driver" activity if the probe request frame has a SSID length of zero, the probe request frame only has a SSID information element frame, and the station fails to proceed with authentication or authorization in response to a probe response frame.

13. A method of detecting an unauthorized station in a wireless local area network engaging in "war driver" activity, the method comprising:

receiving a probe request sent by a station in the wireless local area network;

receiving a probe response frame sent by an access point in the wireless local area network, wherein the probe request frame is sent in response to the probe request frame; and

determining if:

the probe request frame includes a service set identification address ("SSID") with a length of zero,

the probe request frame only has a SSID information element field, and

the station that sent the probe request frame fails to proceed with authentication or authorization in response to the probe response frame.

14. A system of detecting an unauthorized station in a wireless local area network comprising:

an access point configured to send a probe response frame in response to a probe request frame sent from a station; and

a detector configured to:

receive the probe request frame sent from the station, and

analyze the probe request frame to determine if the station is an unauthorized station.

15. The system of claim 14, wherein the detector is configured to:

analyze the probe request frame to determine if the probe request frame has a service set identification address ("SSID") that has a length of zero;

analyze the probe request frame to determine if the probe request frame only has a SSID information element field; and

determine if the station fails to proceed with authentication or authorization in response to the probe response frame.

16. The system of claim 15, wherein the detector is configured to identify the station as an unauthorized station if the probe request frame has a SSID length of zero, the probe request frame only has a SSID information element frame, and the station fails to proceed with authentication or authorization in response to a probe response frame.

17. The system of claim 15, wherein the detector is configured to identify the station as engaging in a war driver activity if the probe request frame has a SSID length of zero, the probe request frame only has a SSID information element frame, and the station fails to proceed with authentication or authorization in response to a probe response frame.

18. The system of claim 14, wherein the detector is a station in the wireless local area network.

19. A computer-readable storage medium containing computer executable code to detect an unauthorized station in a wireless local area network by instruction the computer to operate as follows:

receiving a probe request frame sent from a station at a detector; and

analyzing the probe request frame at the detector to determine if the station is an unauthorized station.

20. The computer-readable storage medium of claim 19, wherein analyzing the probe request frame comprises:

determining if the probe request frame has a service set identification address ("SSID") with a length of zero;

determining if the probe request frame only has a SSID information element field; and

determining if the station fails to proceed with authentication or authorization in response to a probe response frame sent from an access point.

21. The computer-readable storage medium of claim 20 further comprising:

identifying the station as an unauthorized station if the probe request frame has a SSID length of zero, the probe request frame only has a SSID information element frame, and the station fails to proceed with authentication or authorization in response to a probe response frame.

22. The computer-readable storage medium of claim 20 further comprising:

identifying the station as engaging in "war driver" activity if the probe request frame has a SSID length of zero, the probe request frame only has a SSID information element frame, and the station fails to proceed with authentication or authorization in response to a probe response frame.

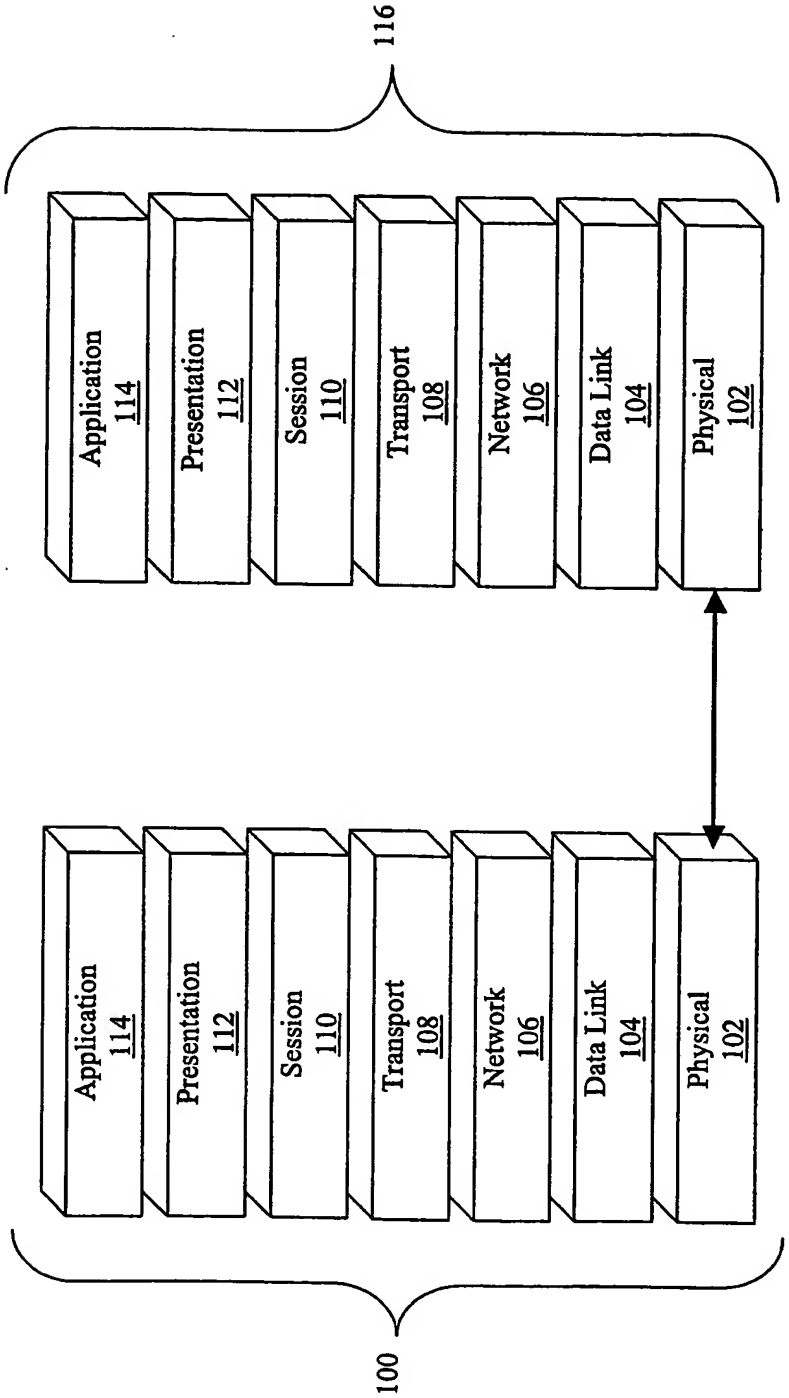

116
Application 114
Presentation 112
Session 110
Transport 108
Network 106
Data Link 104
Physical 102
Application 114
Presentation 112
Session 110
Transport 108
Network 106
Data Link 104
Physical 102
100

Fig. 1

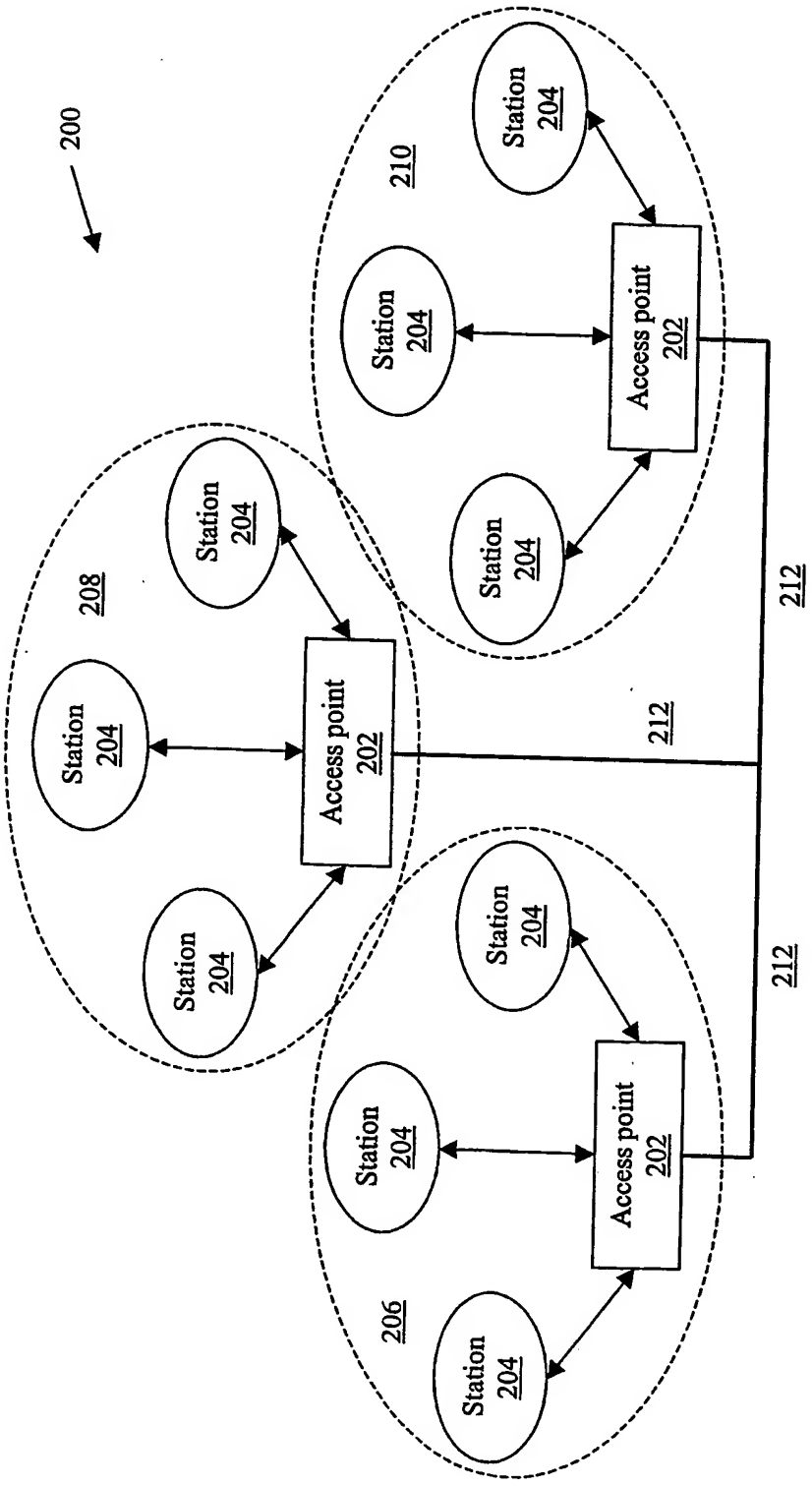


Fig. 2

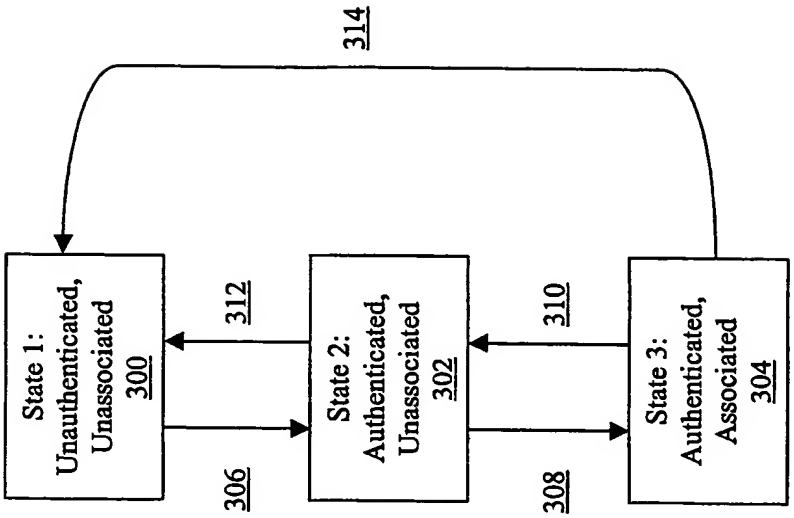

314
State 1: Unauthenticated, Unassociated 300
State 2: Authenticated, Unassociated 302
State 3: Authenticated, Associated 304
312
310
306
308

Fig. 3

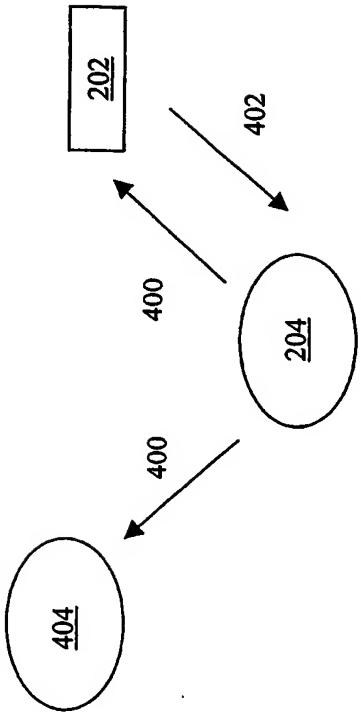


Fig. 4

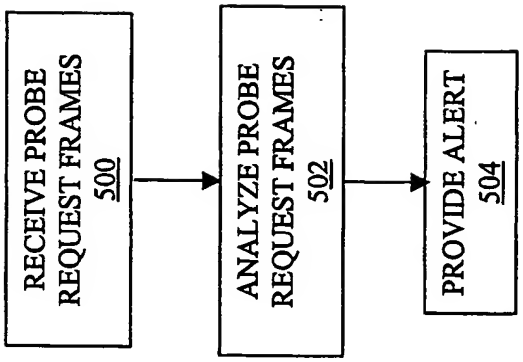

RECEIVE PROBE REQUEST FRAMES 500
ANALYZE PROBE REQUEST FRAMES 502
PROVIDE ALERT 504

Fig. 5

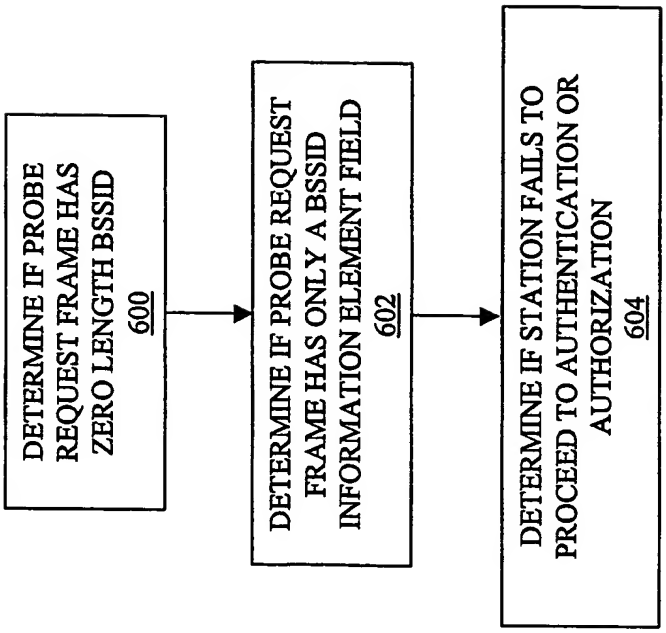

DETERMINE IF PROBE REQUEST FRAME HAS ZERO LENGTH BSSID
600
DETERMINE IF PROBE REQUEST FRAME HAS ONLY A BSSID INFORMATION ELEMENT FIELD
602
DETERMINE IF STATION FAILS TO PROCEED TO AUTHENTICATION OR AUTHORIZATION
604

Fig. 6

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/09682

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 15/173
US CL : 709/224

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 709/224, 223, 217, 229

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
NONE

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6,345,043 B1 (HSU) 05 February 2002, see the whole reference.	1-22
A	US 5,978,919 A (DOI et al) 02 November 1999, see the whole reference.	1-22
A	US 5,982,762 A (ANZAI et al) 09 November 1999, see the whole reference.	1-22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search
12 June 2003 (12.06.2003)

Date of mailing of the international search report
02 JUL 2003

Name and mailing address of the ISA/US
Mail Stop PCT, Attn: ISA/US
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
Facsimile No. (703)305-3230

Authorized officer
Ayaz R Sheikh
Telephone No. 703-305-3900

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

PCT/US03/09682

Continuation of B. FIELDS SEARCHED Item 3:
EAST and WEST
Search terms : wireless LAN, unauthorized, authentication, intrusion, monitoring, detection.